UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/626,103	07/23/2003	Edwin O. Blew	122467.2610	8962

7590 06/29/2006

Pepper Hamilton LLP
One Mellon Center, 50th Floor
500 Grant Street
Pittsburgh, PA 15219

EXAMINER	
ZAND, KAMBIZ	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/626,103	BLEW ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-10,12-16 and 22-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-10,12-16 and 22-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 July 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *07/26/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's election with traverse of Invention I, claims 1-4, 6-10, 12, 13, 22, 23, 34 and 35 in the reply filed on 04/12/2006 is acknowledged. **However due to applicant's persuasive arguments the restriction have been withdrawn and all the claims have been examined.**

2. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.

3. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

4. Claims 5, 11 and 17-21 have been cancelled.

5. Claims 1, 22, 23 and 26 are amended.

6. Claims 1-4, 6-10, 12-16 and 22-35 have been examined.

Drawings

7. The drawings are objected to because of minor informalities: The phrase "103" has been shown in Fig.2. to represent both "network" and "communication" line. Examiner suggests phrase 102" for the "network" in harmony with other Applicant's figures and description. Correction is requested.

Applicant's Priority Claims

8. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. [1] as follows:

Examiner rejects applicant's priority of claims 1-33 based on application 09/343, 921, now abandoned. Applicant's amended specification introducing new matter into the application that has no support in the parent application specification (09/343, 921). The new matters are as follows:

A) "encrypting the data file occurs without assistance from a user and without requiring knowledge of the encryption algorithm by the user" Example: page 2 and 3 paragraph [0007] of the specification.

B) "decrypting the encrypted data file occurs without assistance from a user and without requiring knowledge of the decrypting algorithm by the user" Example: page 3, paragraph [0008] of the specification.

9. The later-filed application must be an application for a patent for an invention, which is also disclosed, in the prior application (the parent or original nonprovisional application or provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the

requirements of the first paragraph of 35 U.S.C. 112. See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994).
The disclosure of the prior-filed application, Application No. 09/343, 921 now, abandoned, fails to provide adequate support or enablement in the manner provided by the first paragraph of 35 U.S.C. 112 for one or more claims of this application. No support for the following limitations :

A) "encrypting the data file occurs without assistance from a user and without requiring knowledge of the encryption algorithm by the user" Example: page 2 and 3 paragraph [0007] of the specification.
B) "decrypting the encrypted data file occurs without assistance from a user and without requiring knowledge of the decrypting algorithm by the user" Example: page 3, paragraph [0008] of the specification.

Information Disclosure Statement PTO-1449

10. The Information Disclosure Statement submitted by applicant on 07/26/2004 has been considered. Please see attached PTO-1449.

Claim Objections

11. **Claims 1 and 26 are** objected to because of the following informalities: typo error. Examiner suggests the following corrections:

Claim 1:

- Changing the phrase "an" second occurrence, to the phrase "the" in the limitation "an electronic data file" of the claim.

Claim 26:

- Replacement of "a" second occurrence (line 2) with "the electronic" in the phrase " a data file".

Claim Rejections - 35 USC § 112

12. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

13. **Claims 1-4,6-10, 12-16 and 21-33** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claims 3, 9, 13 and 24-25, the limitation "re-encrypting data file" phrases makes the claims unclear in relationship with the limitations before that. The limitation before disclose "modifying the decrypted data file". The question is the action of re-encryption

is on the modify data file or is the re-encryption of original data file before modification, that is the data file disclosed in the preamble of claim 1.

Please verify. If the act of re-encryption is on the original data file before the modification, no change has to be done on the claim language, only a confirmation in the response to this office action by applicant will do and the rejection would be withdrawn. However if the action of re-encryption is on the modify decrypted data file, then examiner suggests appropriate amendment to correct the error.

Examiner also would make the following remarks:

Examiner distinguishes between :

a) re-encryption of modify data file (in this instant the original data file may have been modified and encrypted in addition to encryption of the original data file before modification. We deal with two set of data).

b) re-encryption of decrypted modify data file (in this instant the original data is encrypted, decrypted, modified and re-encrypted. We still deal with one set of data).

14. **Claims 2** recites the limitation ""verifying the user is authorized to access" in the claim. There is insufficient antecedent basis for this limitation in the claim. Examiner suggests the phrase "a" instead of the phrase "the" in the above phrase.

15. **Claims 1, 7, 14, 26, 27 and 30** recites the limitation "the algorithm" in the claim. There is insufficient antecedent basis for this limitation in the claim. Examiner suggests the phrase "a" instead of the phrase "the" in the above phrase.

16. **Dependent claims 2-4, 6, 8-10, 12, 13, 15, 16, 21-25, 28, 29 and 31-33** are rejected based on their dependency on the independent claims 1, 7, 14, 26, 27 and 30.

Claim Rejections - 35 USC § 102

17. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

18. Claims **1-3, 6-9, 12-16 and 22-35** rejected under 35 U.S.C. 102(e) as being anticipated by Ote et al (6,023,506 A).

As per claims 1 Ote et al (6,023,506 A) teach a method of securely storing an electronic data file (see fig.2 and 5 and associated text), comprising: transmitting to a computer system, an electronic data file, wherein the computer system comprises a memory subsystem and a plurality of memory locations; encrypting the data file in the memory subsystem; and storing the encrypted data file in the one or more memory locations; wherein encrypting the data file occurs without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file (see

fig.2-6 and associated text; see col.2, lines 54-col.3, lines 32; col.4, lines 17-15, lines 8 where encryption/decryption of the data file, storage of it and automatic encryption/decryption of the data file that corresponds to applicant's "without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file" is disclosed in many instances).

As per claim 2 Ote et al (6,023,506 A) teach the method of claim 1 further comprising, verifying the user is authorized to access the computer system (see fig.6, item 115 and associated text).

As per claims 3 and 9 Ote et al (6,023,506 A) teach the method of claims 1 and 7 respectively further comprising, retrieving the encrypted data file from the one or more memory locations; decrypting the data file; modifying the decrypted data file; re-encrypting the data file; and storing the modified data file in the one or more memory locations, wherein the decrypting and re-encrypting occur without assistance from the user and without requiring the user's knowledge of the algorithm used to encrypt the data file (as applied to claim 1 above; in addition see fig.6 where item 117 decrypt the file and where item 119, 118 would re-encrypt the modified decrypted data file as applied to claim 1 above).

As per claims 6, 12, 29 and 33 Ote et al (6,023,506 A) teach the method of claims 1, 7 respectively wherein the memory subsystem includes random access memory (see

col.4, lines 16-28).

As per claim 7 Ote et al (6,023,506 A) teach a method for securely storing an electronic data file comprising: transmitting to a first computer system, an electronic data file, wherein the first computer system comprises a memory subsystem; encrypting the data file in the memory subsystem; transmitting the encrypted data file to a second computer system having a plurality of memory locations; and storing the encrypted data file in one or more of the plurality of memory locations; wherein encrypting the data file occurs without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file see fig.2-6 and associated text; see col.2, lines 54-col.3, lines 32; col.4, lines 17-15, lines 8 where encryption/decryption of the data file, storage of it and automatic encryption/decryption of the data file that corresponds to applicant's "without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file" is disclosed in many instances).

As per claim 8 Ote et al (6,023,506 A) teach the method of claim 7 further comprising: verifying, the user is authorized to access the first computer system see fig.6, item 1112).

As per claim 13 Ote et al (6,023,506 A) teach the method of claim 7 further comprising: retrieving the encrypted data file from the one or more memory locations; transmitting the encrypted data file to a third computer system; decrypting the data file on the third

computer system; modifying, the encrypted data file; re-encrypting the data file on the third computer system; transmitting the modified data file to the second computer system; and storing the modified data file in the one or more memory locations (see fig.1-6 and associated text).

As per claim 14 Ote et al (6,023,506 A) teach a system for transmitting an electronic data file, comprising: a first computer system for encrypting a data file and decrypting an encrypted data file, the first computer system having a memory subsystem; and second computer system in communication with the first computer system, the second computer system a file having a plurality of memory locations configured to store the encrypted data files, wherein the first computer system configured to: receive the data file from a user device, encrypt the data file in the memory subsystem without interaction from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file, and transmit the encrypted data file to the second computer system, wherein the second computer system is configured to: receive the encrypted data file from the first computer system, and store the encrypted data file in one or more memory locations (see fig.2-6 and associated text; see col.2, lines 54-col.3, lines 32; col.4, lines 17-15, lines 8 where encryption/decryption of the data file, storage of it and automatic encryption/decryption of the data file that corresponds to applicant's "without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file" is disclosed in many instances).

As per claim 15 Ote et al (6,023,506 A) teach the system of claim 14 wherein the second computer system is further configured to: process of the file server further comprises: retrieve the modified data file from the one or more memory locations; and transmitting the encrypted data file from the one or more memory locations; and transmit encrypted data file to the first computer system (see fig.1-6 and associated text).

As per claim 16 Ote et al (6,023,506 A) teach the system of claim 14 wherein the first computer system is further configured to: receive the encrypted data file from the second computer system; and decrypt the encrypted data file in the memory subsystem wherein decrypting the encrypted the data file occurs without interaction from a user and without requiring the user's knowledge of the algorithm used to decrypt the encrypted data file by the user (see fig.2-6 and associated text; see col.2, lines 54-col.3, lines 32; col.4, lines 17-15, lines 8 where encryption/decryption of the data file, storage of it and automatic encryption/decryption of the data file that corresponds to applicant's "without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file" is disclosed in many instances).

As per claim 22 Ote et al (6,023,506 A) teach the method of claim 1 further comprising:
retrieving the encrypted data file from the one or more memory locations;
decrypting the data file; and
providing the user access to the data file, wherein the decrypting occurs without

assistance from the user and without requiring the user's knowledge of the algorithm user to encrypt the data file (see fig.2-6 and associated text; see col.2, lines 54-col.3, lines 32; col.4, lines 17-15, lines 8 where encryption/decryption of the data file, storage of it and automatic encryption/decryption of the data file that corresponds to applicant's "without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file" is disclosed in many instances).

As per claim 23 Ote et al (6,023,506 A) teach the method of claim 7 further comprising: retrieving the encrypted data file from the one or more memory locations; decrypting the data file; and providing the user access to the data file, wherein the decrypting occurs without assistance from the user and without requiring the user's knowledge of the algorithm user to encrypt the data file (see fig.2-6 and associated text; see col.2, lines 54-col.3, lines 32; col.4, lines 17-15, lines 8 where encryption/decryption of the data file, storage of it and automatic encryption/decryption of the data file that corresponds to applicant's "without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file" is disclosed in many instances).

As per claim 24 Ote et al (6,023,506 A) teach the system of claim 14 wherein the second computer system is
further configured to: retrieve the encrypted data file from the one or more memory locations;

decrypt the data file;

modify the decrypted data file;

re-encrypt the data file; and

store the modified data file in the one or more memory locations (see fig.2-6 and associated text; see col.2, lines 54-col.3, lines 32; col.4, lines 17-15, lines 8 where encryption/decryption of the data file, storage of it and automatic encryption/decryption of the data file that corresponds to applicant's "without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file" is disclosed in many instances).

As per claim 25 Ote et al (6,023,506 A) teach the system of claim 14 further comprising:

a third computer system in communication with the second computer,

wherein the second computer system is further configured to:

retrieve the encrypted data tile from the one or more memory locations,

transmit the encrypted data file to the third computer system, receive a modified data file from the third computer system, and store the modified data file in the one or more memory locations, and wherein the third computer system is configured to:

receive the encrypted data file from the second computer, decrypt the data file,

modify the decrypted data file, e-encrypt the data file, and transmit the modified data file to the second computer (see fig.2-6 and associated text; see col.2, lines 54-col.3, lines 32; col.4, lines 17-15, lines 8 where encryption/decryption of the data file, storage of it

and automatic encryption/decryption of the data file that corresponds to applicant's "without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file" is disclosed in many instances).

As per claim 26 Ote et al (6,023,506 A) teach a system for securely storing an electronic data file comprising:

a receiving subsystem configured to receive a data file from a user device',

an encrypting subsystem configured to encrypt the data file;

a plurality of memory locations configured to store an encrypted data file in one or more memory locations; a decrypting subsystem configured to decrypt the encrypted data file; and a display subsystem configured to display the decryption file.

wherein the encrypting subsystem operates to encrypt the data file without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data tile, and wherein the decrypting subsystem operates to decrypt the encrypted data file without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt data file (see fig.2-6 and associated text; see col.2, lines 54-col.3, lines 32; col.4, lines 17-15, lines 8 where encryption/decryption of the data file, storage of it and automatic encryption/decryption of the data file that corresponds to applicant's "without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file" is disclosed in many instances).

As per claim 27 Ote et al (6,023,506 A) teach a method for accessing a secure electronic file on a computer

system, comprising:

retrieving, from a computer system having a memory subsystem and a plurality of memory locations, an encrypted data file from one or more memory locations; decrypting the encrypted data file in the memory subsystem; and providing access to the decrypted data file, wherein decrypting the encrypted data file occurs without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file (see fig.2-6 and associated text; see col.2, lines 54-col.3, lines 32; col.4, lines 17-15, lines 8 where encryption/decryption of the data file, storage of it and automatic encryption/decryption of the data file that corresponds to applicant's "without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file" is disclosed in many instances).

As per claim 28 Ote et al (6,023,506 A) teach the method of claim 27 further comprising:

modifying the decrypted data file; encrypting the modified data file; and

storing the encrypted modified data file in the one or more memory locations,

wherein the encryption of the modified data file occurs without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file (see fig.2-6 and associated text; see col.2, lines 54-col.3, lines 32; col.4, lines 17-15, lines 8 where encryption/decryption of the data file, storage of it and automatic

encryption/decryption of the data file that corresponds to applicant's "without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file" is disclosed in many instances).

As per claim 30 Ote et al (6,023,506 A) teach a method for securely accessing an electronic data file

comprising: retrieving, from a first computer system comprising a plurality of memory locations, an encrypted data file from one or more of the memory locations, transmitting the encrypted data file to a second computer system comprising a memory subsystem; decrypting the encrypted data file in the memory subsystem; and displaying the decrypted data file, wherein decrypting the encrypted data file occurs without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file (see fig.2-6 and associated text; see col.2, lines 54-col.3, lines 32; col.4, lines 17-15, lines 8 where encryption/decryption of the data file, storage of it and automatic encryption/decryption of the data file that corresponds to applicant's "without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file" is disclosed in many instances).

As per claim 31 Ote et al (6,023,506 A) teach the method of claim 30 further comprising:

transmitting the encrypted data file to a third computer system;

decrypting the encrypted data file; modifying, by the third computer system, the data file;

encrypting the modified data file; transmitting the encrypted modified data file to the first computer system; and storing the modified data file in the one or more memory locations (see fig.1-6 and associated text).

As per claim 32 Ote et al (6,023,506 A) teach the method of claim 30 further comprising:

retrieving the encrypted data file from the one or more memory locations,

decrypting the encrypted data file;

modifying the data file; encrypting the modified data file; and

storing the encrypted modified data file in the one or more memory locations (see fig.1-6 and associated text).

As per claim 34 Ote et al (6,023,506 A) teach a system for securely storing electronic data files (see fig.2-3 and associated text) comprising:

means for receiving a data file (see fig.5, item 1030 and associated text with respect to fig.5 where data file received by encryption/decryption means module); means for encrypting the data file (see fig.5 and associated text, item 1000); means for retrieving the stored data file (see col.2, lines 8-64); means for decrypting the retrieved data file (see fig.5, item 1000 and associated text); and

means for displaying the decrypted data tile (see fig.2, item 2 and associated text).

Also see the entire reference for more example of the above limitation.

As per claim 35 Ote et al (6,023,506 A) teach the method of claim 34 further comprising:

means for modifying the retrieved data file (see col.6, lines 31-38; means for encrypting the modified data file; and means for storing the encrypted modified data file (see col.11, lines 32-col.14, lines43 for number of examples in that respect).

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

20. **Claims 4, 10** are rejected under 35 U.S.C. 103(a) as being unpatentable over Ote et al (6,023,506 A).

As per claims 4 and 10 transmitting/receiving information performed using a SSL/HTTPS protocol is well known in the art.

Allowable Subject Matter

21. **Claims 3, 9, 13, 24, 25, 28, , 31 and** is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

22. **Claims 5-7** would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

U.S.Patent No. US (5,623,637 A) teach encrypted data storage card including smartcard integrated circuit for strong and access password and encryption keys.
U.S.Patent No. US (6,115,040 A) teach graphical user interface for web-enabled applications.

Please see enclosed PTO-892 for other related art in addition to the above.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KAMBIZ ZAND
PRIMARY EXAMINER

06/26/2006